Adán Cabello*

*Departamento de Física Aplicada II, Universidad de Sevilla, 41012 Sevilla, Spain*

(September 9, 2000)

A general proof of the security against eavesdropping of a previously introduced protocol for two-party quantum key distribution based on entanglement swapping [Phys. Rev. A **61**, 052312 (2000)] is provided. In addition, the protocol is extended to permit multiparty quantum key distribution and secret sharing of classical information.

PACS numbers: 03.67.Dd, 03.67.Hk, 03.65.Bz

## I. INTRODUCTION

Entanglement swapping (ES), that is, entangling a set of particles $S$ by appropriately projecting other particles previously entangled with particles of $S$ [1–5], has found a number of applications in quantum information: constructing a quantum telephone exchange, speeding up the distribution of entanglement, correcting errors in Bell states, and preparing entangled states of a higher number of particles [3,5]. Recently, ES has also been used to solve the problem of cryptographic key distribution between two parties in an essentially new way [6]. In this paper, the scheme of Ref. [6] is extended to permit the distribution of the same key to several users (multiparty key distribution), and to permit the distribution of the same key to several users in such a way that they must cooperate to obtain the key (secret sharing of classical information). The structure of the paper is the following: In Sec. II A the protocol for quantum key distribution between two parties based on ES is reviewed. A general proof of its security is provided in Sec. II B. Multiparty key distribution is introduced, and a new protocol using Greenberger-Horne-Zeilinger (GHZ) states [7] is presented in Sec. III A. In Sec. III B a different approach, based on ES and which is a generalization the two-party protocol, is introduced. Secret sharing is treated in Sec. IV. Two previous protocols for secret sharing using, respectively, GHZ and Bell states are reviewed in Secs. IV A and IV B. In Sec. IV C, it is shown how the scheme of three-party key distribution based on ES described in Sec. III B, also permits secret sharing. The case of more than three users is treated in Sec. V. Sec. VI is dedicated to demonstrate the security of ES-based protocols against eavesdropping. Finally, the main advantages of these protocols are summarized in Sec. VII.

*Electronic address: adan@cica.es, fite1z1@sis.ucm.es

## II. QUANTUM KEY DISTRIBUTION BETWEEN TWO PARTIES

### A. The protocol based on entanglement swapping

The key distribution problem of cryptography is the following: Alice wishes to convey a sequence of random classical bits (a “key”) to Bob, while preventing that Eve acquires information without being detected. This problem, which has no solution by classical means, can be solved using quantum mechanics [8]. Indeed, subsequent developments have shown that quantum mechanics provides different tools to solve the problem. Some are based on the impossibility of cloning unknown nonorthogonal quantum states [8,9], some also use entanglement between two particles [10,11], some combine quantum techniques with classical private amplification and compression techniques [12], and some are based on splitting the information in several qubits to which Eve has only a sequential access [13–15]. In Ref. [6], a new method for key distribution based on ES was introduced. Let us start by briefly reviewing how this ES-based protocol works. Consider the orthonormal basis of Bell states given by:

$$|00\rangle_{ij} = \frac{1}{\sqrt{2}}\left(|0\rangle_i \otimes |0\rangle_j + |1\rangle_i \otimes |1\rangle_j\right), \tag{1}$$

$$|01\rangle_{ij} = \frac{1}{\sqrt{2}}\left(|0\rangle_i \otimes |0\rangle_j - |1\rangle_i \otimes |1\rangle_j\right), \tag{2}$$

$$|10\rangle_{ij} = \frac{1}{\sqrt{2}}\left(|0\rangle_i \otimes |1\rangle_j + |1\rangle_i \otimes |0\rangle_j\right), \tag{3}$$

$$|11\rangle_{ij} = \frac{1}{\sqrt{2}}\left(|0\rangle_i \otimes |1\rangle_j - |1\rangle_i \otimes |0\rangle_j\right), \tag{4}$$

where

$$\sigma_z\,|0\rangle = |0\rangle\,, \tag{5}$$

$$\sigma_z\,|1\rangle = -\,|1\rangle\,, \tag{6}$$

being $\sigma_z$ the corresponding Pauli spin matrix. For convenience, we shall divide the protocol in three parts:

(I) *Preparation.* Initially, Alice has four qubits: qubits 1 and 2, prepared in one public Bell state of the basis (1)-(4), and qubits 3 and 5, prepared in another Bell public state of the same basis. Bob, in a distant place, has two qubits, 4 and 6, prepared in a public Bell state of the same basis. For example, the initial state of the six qubits can be

$$|\Psi_I\rangle = |00\rangle_{12} \otimes |00\rangle_{35} \otimes |00\rangle_{46}\,. \tag{7}$$

Next, Alice sends qubit 2 out to Bob through an insecure quantum channel (i.e., Eve can manipulate qubit 2).

(II) *Generation of two bits of the key.* Alice performs a complete Bell-state measurement on qubits 1 and 3 (henceforth referred to as Alice's *secret* measurement). The result, $AS$ (a random number: "00" if the result is $|00\rangle$, "01" if it is $|01\rangle$, "10" if it is $|10\rangle$, or "11" if it is $|11\rangle$), defines two bits of the key. Then, the state is

$$|\Psi_{II}\rangle = |AS\rangle_{13} \otimes |AS'\rangle_{25} \otimes |00\rangle_{46}\,, \tag{8}$$

where $|AS'\rangle$ is a Bell state which is in one-to-one correspondence with $|AS\rangle$.

(III) *How Bob obtains the two bits of the key.* Bob performs a complete Bell-state measurement on qubits 2 and 4 (henceforth referred to as Bob's *secret* measurement), and keeps the result, $BS$, secret. After that, the state is

$$|\Psi_{III}\rangle = |AS\rangle_{13} \otimes |BS\rangle_{24} \otimes |AP\rangle_{56}\,, \tag{9}$$

where $|AP\rangle$ is a Bell state which can be determined from the pair $AS$, $BS$. Then, Bob sends qubit 6 out to Alice (i.e., Eve can manipulate qubit 6). Finally, Alice performs a complete Bell-state measurement on qubits 5 and 6 (henceforth referred to as Alice's *public* measurement), and publicly announces the result, $AP$, through a classical channel (which is assumed to be public but which cannot be altered) [16]. Due to the successive ES between the pairs of qubits, for each of the four possible values of $AP$, there is a different one-to-one correspondence between the results of Alice's and Bob's secret measurements. These correspondences are compiled in Table I. Therefore, once Bob knows the $AP$, he can infer $AS$. The process must be sequentially repeated until the key is large enough.

### B. Security of the protocol based on ES

In Ref. [6], the security against eavesdropping of the protocol for two-party key distribution based on ES was showed for a particular eavesdropping attack. Here I will provide a general (i.e., attack-independent) proof.

The result $AS$ defines two bits of the key. However, $AS$ is random and Eve cannot influence it by manipulating any of the transmitted qubits. To obtain $AS$, Eve needs the same two ingredients as Bob: $BS$ and $AP$. In addition, to avoid being detected, Eve needs to obtain $BS$ *without changing* $AP$. However, since Eve has only access to two of the six qubits, we shall see that any procedure that allows Eve to obtain $BS$, changes $AP$ in an unpredictable way. Let us examine the strategies that Eve can follow and their consequences.

In step (I) of the protocol, the only qubit accessible to Eve is qubit 2. If Eve's aim is to obtain $BS$ (as a previous step to obtain $AS$), the only useful strategy is one whose result is equivalent to capturing qubit 2 and substituting it by an ancillary qubit 8 (which will be sent out to Bob), which was previously prepared in a Bell state (for instance $|00\rangle_{78}$) with another ancillary qubit 7 (which will be retained by Eve) [17]. After this manœuvre the state of the qubits is

$$|\Psi'_{I}\rangle = |00\rangle_{12} \otimes |00\rangle_{35} \otimes |00\rangle_{46} \otimes |00\rangle_{78}\,, \tag{10}$$

where Alice has qubits 1, 3, and 5; Bob has qubits 4, 6, and 8; and Eve has qubits 2 and 7. This situation is illustrated in Fig. 1 (a1). The corresponding situation in the alternative scenario in which Eve is not present is illustrated in Fig. 1 (b1).

In step (II), Alice performs her secret measurement on qubits 1 and 3, and Bob performs his secret measurement on qubits 4 and 8 (which substitutes qubit 2). After these measurements the state of the qubits is

$$|\Psi'_{II}\rangle = |AS\rangle_{13} \otimes |AS'\rangle_{25} \otimes |BS'\rangle_{67} \otimes |BS\rangle_{48}\,, \tag{11}$$

where $|AS\rangle$ is the Bell state which defines two bits of the key, $|AS'\rangle$ is a Bell state in one-to-one correspondence with $|AS\rangle$, $|BS\rangle$ is the Bell state which gives Bob's secret result $BS$, and $|BS'\rangle$ is a Bell state in one-to-one correspondence with $|BS\rangle$. This situation is illustrated in Fig. 1 (a2). The corresponding situation in the alternative scenario in which Eve is not present is illustrated in Fig. 1 (b2).

In the step (III), Bob sends qubit out 6 to Alice. This allows Eve to capture it and obtain $BS$ by performing a Bell-state measurement on qubits 6 and 7 (the result $BS'$ of this measurement is in one-to-one correspondence with $BS$). This is (modulo equivalencies) the only strategy that allows Eve to obtain $BS$. Now, to obtain $AS$, she still needs to know $AP$ (which must be in one-to-one correspondence with the pair $AS$, $BS$). However, Eve's intervention has changed the state of the qubits (compare $|\Psi_{II}\rangle$ with $|\Psi'_{II}\rangle$).

Before Alice's public measurement, Eve has access to qubit 2 (which is in a Bell state, unknown to Eve, with Eve's qubit 5), and to qubits 6 and 7. If Eve manages to give Alice a qubit in the Bell state $|AP\rangle$ with qubit 2, then her intervention won't be detected. Eve can prepare a qubit in any desired Bell state with qubit 2; the problem is that she does not know which is the "correct" Bell state. Indeed, she cannot know which is the right one since this would require Eve to know $|AS\rangle_{13}$ (and Eve has no access to qubits 1 and 3), or $|AS'\rangle_{25}$ (and Eve only has access to qubit 2, and since the partial trace of all the Bell states is the identity matrix, any measurement on one qubit cannot reveal anything about the state of both qubits).

Alternatively, if Eve gives to Alice qubit 6 (or 7), then the result of Alice's public measurement will allow Eve to obtain $AS'$ (and therefore $AS$). However, this result is not in one-to-one correspondence with the pair $AS$, $BS$ anymore. Therefore, the result obtained by Alice will be the "wrong" one in $\frac{3}{4}$ of the runs, and thus Eve's intervention can be detected when Alice and Bob compare subsets of their keys.

Summing up, no strategy allows Eve to extract information without being detected, because the only strategy that Eve can use to obtain information will change the expected result for $AP$ in $\frac{3}{4}$ of the cases. In addition, this proves that one of the interesting features of the protocol based on ES —namely, that it improves the efficiency of the detection of eavesdropping compared with other protocols [6]— is independent of the attack.

## III. MULTIPARTY KEY DISTRIBUTION

### A. Multiparty key distribution using two GHZ states

Consider the following problem: Alice wishes to convey the *same* key to $N$ users (Bob, Carol,..., Nathan), while preventing Eve from acquiring information without being detected. This problem, called *multiparty key distribution*, is a special case of networked *cryptographic conferencing* [18,19].

Here I introduce a protocol for using GHZ states for multiparty quantum key distribution that, as far as I know, has not been presented anywhere before. It can be considered as a generalization to many parties of the two-party protocol of Ref. [10].

Let us focus our attention in the case $N = 3$ (the cases with $N > 3$ are straightforward extensions of this case). Alice wishes to distribute the same key to Bob and Carol. For that purpose, she randomly prepares one of the following two three-qubit GHZ states:

$$|\psi_z\rangle_{ijk} = \frac{1}{\sqrt{2}}(|0\rangle_i \otimes |0\rangle_j \otimes |0\rangle_k + |1\rangle_i \otimes |1\rangle_j \otimes |1\rangle_k), \tag{12}$$

$$|\psi_x\rangle_{ijk} = \frac{1}{\sqrt{2}}(|\bar{0}\rangle_i \otimes |\bar{0}\rangle_j \otimes |\bar{0}\rangle_k + |\bar{1}\rangle_i \otimes |\bar{1}\rangle_j \otimes |\bar{1}\rangle_k), \tag{13}$$

where

$$\sigma_x |\bar{0}\rangle = |\bar{0}\rangle, \tag{14}$$

$$\sigma_x |\bar{1}\rangle = -|\bar{1}\rangle, \tag{15}$$

being $\sigma_x$ the corresponding Pauli spin matrix. Then Alice sends one of the three qubits out to Bob, another to Carol, and retains the third one. Bob and Carol perform a measurement of either $\sigma_z$ or $\sigma_x$ on their own qubit. When Alice has prepared the state $|\psi_z\rangle$ ($|\psi_x\rangle$), and both Bob and Carol have measured $\sigma_z$ ($\sigma_x$) —i.e., in $\frac{1}{4}$ of the cases—, all of them obtain the same result. In that case, they can use this result to define one bit of the key. The other cases are not useful for establishing a common key and are rejected. Alternatively, to reduce the wastage of qubits due to the noncoincidence of the measurements, Alice can tell Bob and Carol which is the "right" measurement (once all three qubits are safe from Eve's intervention). The security of this scheme against eavesdropping is guaranteed by the impossibility of cloning an unknown state chosen between $|\psi_z\rangle$ and $|\psi_x\rangle$, specially when Eve only has access to two of the three qubits.

### B. Multiparty key distribution based on entanglement swapping

A different multiparty key distribution protocol can be obtained using ES. Indeed, what follows is just one of the possible generalizations to three parties of the protocol for key distribution between two parties based on ES of Ref. [6].

Consider the orthonormal basis of GHZ states given by:

$$|000\rangle_{ijk} = \frac{1}{\sqrt{2}}(|0\rangle_i \otimes |0\rangle_j \otimes |0\rangle_k + |1\rangle_i \otimes |1\rangle_j \otimes |1\rangle_k), \tag{16}$$

$$|001\rangle_{ijk} = \frac{1}{\sqrt{2}}(|0\rangle_i \otimes |0\rangle_j \otimes |0\rangle_k - |1\rangle_i \otimes |1\rangle_j \otimes |1\rangle_k), \tag{17}$$

$$|010\rangle_{ijk} = \frac{1}{\sqrt{2}}(|0\rangle_i \otimes |0\rangle_j \otimes |1\rangle_k + |1\rangle_i \otimes |1\rangle_j \otimes |0\rangle_k), \tag{18}$$

$$|011\rangle_{ijk} = \frac{1}{\sqrt{2}}(|0\rangle_i \otimes |0\rangle_j \otimes |1\rangle_k - |1\rangle_i \otimes |1\rangle_j \otimes |0\rangle_k), \tag{19}$$

$$|100\rangle_{ijk} = \frac{1}{\sqrt{2}}(|0\rangle_i \otimes |1\rangle_j \otimes |0\rangle_k + |1\rangle_i \otimes |0\rangle_j \otimes |1\rangle_k), \tag{20}$$

$$|101\rangle_{ijk} = \frac{1}{\sqrt{2}}(|0\rangle_i \otimes |1\rangle_j \otimes |0\rangle_k - |1\rangle_i \otimes |0\rangle_j \otimes |1\rangle_k), \tag{21}$$

$$|110\rangle_{ijk} = \frac{1}{\sqrt{2}}(|1\rangle_i \otimes |0\rangle_j \otimes |0\rangle_k + |0\rangle_i \otimes |1\rangle_j \otimes |1\rangle_k), \tag{22}$$

$$|111\rangle_{ijk} = \frac{1}{\sqrt{2}}(|1\rangle_i \otimes |0\rangle_j \otimes |0\rangle_k - |0\rangle_i \otimes |1\rangle_j \otimes |1\rangle_k). \tag{23}$$

The protocol can be summarized in four steps, which are illustrated in Fig. 2:

(i) Initially, Alice has qubits 1 and 2, prepared in one public Bell state of the basis (1)-(4), and qubits 3, $A$, and $B$ (qubits described by numbers stay with the same user during all the protocol, and qubits described by letters are transmitted between users during the protocol) prepared in a GHZ state of the basis (16)-(23). Bob (Carol), in a distant place, has two qubits, 5 and $D$ (4 and $C$), prepared in a public Bell state. For instance, the initial state of the nine qubits can be

$$|\psi_i\rangle = |000\rangle_{3AB} \otimes |00\rangle_{12} \otimes |00\rangle_{5D} \otimes |00\rangle_{4C}, \tag{24}$$

where subindexes 3, $A$, etc., mean qubits 3, $A$, etc.

(ii) Then, Alice sends qubit $A$ ($B$) out to Bob (Carol) through an insecure quantum channel. Next, Alice performs a secret Bell-state measurement on qubits 2 and 3, Bob performs a secret Bell-state measurement on qubits 5 and $A$, and Carol performs a secret Bell-state measurement on qubits 4 and $B$.

(iii) After these three secret measurements, the state of qubits 1, $C$, and $D$ becomes a GHZ state of the basis (16)-(23), due to multiparticle ES [3]. The final state is

$$|\psi_{iii}\rangle = |AP\rangle_{1CD} \otimes |AS\rangle_{23} \otimes |BS\rangle_{5A} \otimes |CS\rangle_{4B} . \quad (25)$$

(iv) Then, Bob (Carol) sends qubit $D$ ($C$) out to Alice, who performs a complete GHZ-state measurement on qubits 1, $C$, and $D$ [i.e., a measurement which unambiguously discriminates between states (16)-(23)], and publicly announces the result through a classical channel.

Out of the 512 possible combinations of results (for Alice's public measurement, and Alice's, Bob's, and Carol's secret measurements), there are only 64 which have a nonzero probability to occur. If the initial state is (24), these 64 combinations are represented in Table II. All of them have the same probability to occur ($\frac{1}{64}$).

The secret key that Alice, Bob, and Carol will share is defined as the *first* bit of Alice's secret measurement. As a close examination of Table II reveals, Bob (or Carol) can infer Alice's first bit using just two ingredients: the result of the public measurement, and the result of his (her) own secret measurement. Therefore, once Bob (Carol) knows the result of the public measurement, he (she) can infer the first bit of the result of Alice's secret measurement. The process can be sequentially repeated.

## IV. QUANTUM SECRET SHARING OF CLASSICAL INFORMATION

### A. Hillery-Bužek-Berthiaume secret sharing using GHZ states

Consider the following problem: Alice wishes to convey a key to Bob and Carol in such a way that none of them can read it on their own, only if they collaborate. In addition, they wish to prevent that Eve acquires information without being detected. This is an interesting problem in the following scenario [20]: Alice wants to have a secret action taken on her behalf in a distant part. There she has two agents, Bob and Carol, who carry it out for her. Alice knows that one and only one of them is dishonest, but she does not know which one. She cannot simply send a secure message to both of them, because the dishonest one will try to sabotage the action, but she knows that if both carry it out together, the honest one will keep the dishonest one from doing any damage.

A first solution to this problem using quantum tools was provided in Ref. [20], and can be summarized as follows: Alice prepares three qubits in the GHZ state given by Eq. (12), and sends one qubit out to Bob, another to Carol, and keeps the third. Bob and Carol independently and randomly choose whether to measure $\sigma_x$ or $\sigma_y$ on their qubits. They then publicly announce which measurement they have made, but not which result they have obtained. If Bob and Carol have chosen the same measurement, they can then determine what was the result of Alice's measurement by combining their results. This allows Alice, Bob, and Carol to establish a common key. The other events in which Bob and Carol have chosen different measurements (which are $\frac{1}{2}$ of the events) do not allow them to make useful inferences to establish a key and are therefore rejected. For details on this protocol and for proofs of its security see [20,21].

### B. Karlsson-Koashi-Imoto secret sharing using Bell states

In Ref. [21] another protocol for secret sharing using Bell states instead of GHZ states is proposed. It works as follows: Alice prepares two qubits in one of the following four states:

$$\begin{aligned} |\psi^+\rangle_{ij} &= \frac{1}{\sqrt{2}}\left(|0\rangle_i \otimes |0\rangle_j + |1\rangle_i \otimes |1\rangle_j\right) \\ &= \frac{1}{\sqrt{2}}\left(|\bar{0}\rangle_i \otimes |\bar{0}\rangle_j - |\bar{1}\rangle_i \otimes |\bar{1}\rangle_j\right), \quad (26) \\ |\phi^-\rangle_{ij} &= \frac{1}{\sqrt{2}}\left(|0\rangle_i \otimes |0\rangle_j - |1\rangle_i \otimes |1\rangle_j\right) \\ &= \frac{1}{\sqrt{2}}\left(|\bar{0}\rangle_i \otimes |\bar{1}\rangle_j + |\bar{1}\rangle_i \otimes |\bar{0}\rangle_j\right), \quad (27) \\ |\Psi^+\rangle_{ij} &= \frac{1}{\sqrt{2}}\left(|0\rangle_i \otimes |\bar{0}\rangle_j + |1\rangle_i \otimes |\bar{1}\rangle_j\right) \\ &= \frac{1}{\sqrt{2}}\left(|\bar{0}\rangle_i \otimes |0\rangle_j + |\bar{1}\rangle_i \otimes |1\rangle_j\right), \quad (28) \\ |\Phi^-\rangle_{ij} &= \frac{1}{\sqrt{2}}\left(|0\rangle_i \otimes |\bar{1}\rangle_i - |1\rangle_i \otimes |\bar{0}\rangle_j\right) \\ &= \frac{1}{\sqrt{2}}\left(|\bar{0}\rangle_i \otimes |1\rangle_j - |\bar{1}\rangle_i \otimes |0\rangle_j\right), \quad (29) \end{aligned}$$

and sends out one of the qubits to Bob and the other to Carol. They independently and randomly perform a measurement of either $\sigma_z$ or $\sigma_x$. Then Bob and Carol have a public discussion where they declare the measurement outcomes for a subset of bits used for testing eavesdropping. It is essential that this discussion takes place before any further declaration. If they do not detect eavesdropping, Bob publicly declares the outcomes of his measurements (but not yet his choice of measurements), then Carol declares both her choice of measurements and the corresponding outcomes, and finally Bob declares his choice of measurements (the order of the declarations is important to preserve security). Then, Alice publicly reveals whether she has prepared one of the states $\{|\psi^+\rangle, |\phi^-\rangle\}$, or one of the states $\{|\Psi^+\rangle, |\Phi^-\rangle\}$

(but not which specific state she has prepared). If Alice has prepared a state of the first (second) set, then the results of Bob's and Carol's local measurements are correlated only if both have chosen to measure $\sigma_z$ or both have chosen to measure $\sigma_x$ (if one of them has chosen to measure $\sigma_z$ and the other has chosen to measure $\sigma_x$). Such correlations allow Bob and Carol to find out which state Alice has prepared. But this is only possible if both cooperate. Note that in this protocol, in half of the events there is no correlation between Bob's and Carol's results so half of the events are not useful for secret sharing and must be rejected.

### C. Secret sharing using entanglement swapping

In Sec. III B we saw how to distribute one bit between three users employing ES between two-qubit Bell states and three-qubit GHZ states. In this section we show that the scenario described there also allows secret sharing of classical information. The protocol for secret sharing has steps (i) to (iii) in common with the protocol of multiparty key distribution described in Sec. III B. In step (iv), we saw that once Bob (Carol) knows the result of the public measurement, he (she) can infer the *first* bit of the result of Alice's secret measurement. In addition, as a close inspection of Table II shows, once Bob (Carol) knows the result of Carol's (Bob's) secret measurement, he (she) can infer the *second* bit of the result of Alice's secret measurement. That is, if Bob and Carol cooperate they can infer this second bit. Therefore, the same scenario allows us to develop a protocol for multiparty key distribution and, simultaneously, a protocol for secret sharing.

## V. ES-BASED PROTOCOL FOR MULTIPARTY KEY DISTRIBUTION AND SECRET SHARING BETWEEN MORE THAN THREE USERS

Both the scheme for multiparty key distribution based on ES, described in Sec. III B, and the scheme for secret sharing described in Sec. IV C, can be extended to $N$ users as follows:

(i) Every user has a pair of qubits in a public Bell state. In addition, Alice has another $N$ qubits prepared in a GHZ state of the orthonormal basis:

$$\begin{aligned} |00...0\rangle_{ij...N} &= \frac{1}{\sqrt{2}}(|0\rangle_i \otimes |0\rangle_j \otimes ... \otimes |0\rangle_N + \\ &\quad |1\rangle_i \otimes |1\rangle_j \otimes ... \otimes |1\rangle_N), \quad (30) \\ |00...1\rangle_{ij...N} &= \frac{1}{\sqrt{2}}(|0\rangle_i \otimes |0\rangle_j \otimes ... \otimes |0\rangle_N - \\ &\quad |1\rangle_i \otimes |1\rangle_j \otimes ... \otimes |1\rangle_N), \quad (31) \\ &... \\ |11...0\rangle_{ij...N} &= \frac{1}{\sqrt{2}}(|1\rangle_i \otimes |0\rangle_j \otimes ... \otimes |0\rangle_N + \\ &\quad |0\rangle_i \otimes |1\rangle_j \otimes ... \otimes |1\rangle_N), \quad (32) \\ |11...1\rangle_{ij...N} &= \frac{1}{\sqrt{2}}(|1\rangle_i \otimes |0\rangle_j \otimes ... \otimes |0\rangle_N - \\ &\quad |0\rangle_i \otimes |1\rangle_j \otimes ... \otimes |1\rangle_N). \quad (33) \end{aligned}$$

For instance, consider that the initial state of the system is

$$|\Psi_i\rangle = |00...0\rangle \otimes |00\rangle \otimes ... \otimes |00\rangle \,. \quad (34)$$

(ii) Then, Alice sends a qubit of her GHZ state out to each of the other $N-1$ users. Next, each user (including Alice) performs a Bell-state measurement on the received qubit and one of their qubits.

(iii) After these measurements the state of the system becomes

$$|\Psi_{iii}\rangle = |AP\rangle \otimes |AS\rangle \otimes |BS\rangle \otimes ... \otimes |NS\rangle \,, \quad (35)$$

where $|AP\rangle$ is a $N$-qubit GHZ state of the basis (30)-(33), and the ordering of the qubits is not the same as in $|\Psi_i\rangle$ (as occurs in Secs. II A and III B).

(iv) Then, the $N-1$ users sends a qubit (the one they have no used) to Alice, and she performs a measurement to discriminate between the $2^N$ GHZ states (30)-(33), and publicly announces the result. This result $AP$, and the result of their own secret measurement allow each legitimate user to infer the first bit of Alice's secret result $AS$. To find out the second bit of $AS$, *all* users (except Alice) must cooperate. For instance, in case there are four users (Alice, Bob, Carol, and David), to obtain the second bit of $AS$ it is not enough that Bob and Carol share their secret results. As Table III shows, they also need to know David's secret result.

## VI. SECURITY OF THE PROTOCOLS BASED ON MULTIPARTICLE ES

The proof of the security against eavesdropping of the protocols for multiparty key distribution and secret sharing based on multiparticle ES is parallel to the one developed in Sec. II B for the protocol for two parties key distribution. The guidelines of the proof are the following:

$AS$ (whose first bit defines the part of the key that the legitimate users can obtain without cooperating, and whose second bit defines the part of the key that the users can obtain if they cooperate) is a random number, and Eve cannot do anything to change or influence it.

In order to obtain the first (second) bit of $AS$, Eve needs the same ingredients that any legitimate user needs: the result of the secret measurement of one (all) of them, and $AP$.

Any attempt to find out one of the secret results will change the result $AP$ in an unpredictable way. Therefore, Eve's presence can be detected. Indeed, detecting Eve requires the comparison of fewer bits than in other protocols since the probability that the result $AP$ is a "wrong" one is $\frac{2^N-1}{2^N}$, being $N$ the number of users.

## VII. CONCLUSIONS

The main aim of this paper has been to introduce new protocols for multiparty key distribution and secret sharing of classical information. The main interest of the protocols based on ES is that they provide a conceptually different way to solve certain problems of information theory. Its main advantages are that no transmitted quantum data are rejected, so they improve the efficiency of previous protocols; and that the detection of Eve requires the comparison of fewer bits, since the probability that Eve alters the result expected by the legitimate users is higher. On the other hand, since these protocols involve complete Bell-state and GHZ-state discriminations, they are much more difficult to perform in practice than previous protocols based on simpler measurements.

In this paper we have focused our attention in the distribution of classical information. However, as occurs with previous proposals, the protocols presented here can also be used, with little modifications, to distribute quantum information [3,20] and for secret sharing of quantum information [20–23].

## ACKNOWLEDGMENTS

The author thanks S. Bose for useful discussions on multiparty key distribution and the organizers of the Sixth Benasque Center for Physics, the University of Seville, and the Junta de Andalucía for support.

[1] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[2] M. Żukowski, A. Zeilinger, M.A. Horne, and A.K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).
[3] S. Bose, V. Vedral, and P.L. Knight, Phys. Rev. A **57**, 822 (1998).
[4] J-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998).
[5] S. Bose, V. Vedral, and P.L. Knight, in *The Physics of Quantum Information*, edited by D. Bouwmeester, A.K. Ekert, and A. Zeilinger (Springer, Berlin, 2000).
[6] A. Cabello, Phys. Rev. A **61**, 052312 (2000).
[7] D.M. Greenberger, M.A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer, Dordrecht, 1989), p. 69.
[8] C.H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[9] C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[10] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[11] C.H. Bennett, G. Brassard, and N.D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[12] H.-K. Lo and H.F. Chau, US Patent 5732139 (1998); M. Ardehali, H.F. Chau, and H.-K. Lo, quant-ph/9803007 (unpublished).
[13] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
[14] M. Koashi and N. Imoto, Phys. Rev. Lett. **79**, 2383 (1997).
[15] A. Cabello, quant-ph/0007064.
[16] In this protocol, the results of the public measurement play the same role as Alice's choice between bases in the protocol of Ref. [8]. Therefore, in addition to those mentioned in Ref. [6], one interesting feature of the protocol based on ES is that the "choice" of basis is truly random, and therefore it does not require any specific set-up to randomize it.
[17] Steps 1 and 2 of the particular attack discussed in Ref. [6] are equivalent to this procedure.
[18] S.J.D. Phoenix, S.M. Barnett, P.D. Townsend, and K.J. Blow, J. Mod. Opt. **42**, 1155 (1995); P.D. Townsend, C. Marand, S.J.D. Phoenix, K.J. Blow, and S.M. Barnett, Philos. Trans. R. Soc. London, Ser. A **354**, 805 (1996); P.D. Townsend, Nature (London) **385**, 47 (1997).
[19] E. Biham, B. Huttner, and T. Mor, Phys. Rev. A **54**, 2651 (1996).
[20] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[21] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
[22] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[23] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).

| Public | Alice | Bob | Public | Alice | Bob |
|---|---|---|---|---|---|
| 00 | 00 | 00 | 10 | 00 | 10 |
| ” | 01 | 01 | ” | 01 | 11 |
| ” | 10 | 10 | ” | 10 | 00 |
| ” | 11 | 11 | ” | 11 | 01 |
| 01 | 00 | 01 | 11 | 00 | 11 |
| ” | 01 | 00 | ” | 01 | 10 |
| ” | 10 | 11 | ” | 10 | 01 |
| ” | 11 | 10 | ” | 11 | 00 |

TABLE I. The 16 possible combinations of results of Alice's public Bell-state measurement, and Alice's and Bob's secret Bell-state measurements on the initial state given by Eq. (7).

| Public | Alice | Bob | Carol | Public | Alice | Bob | Carol |
|---|---|---|---|---|---|---|---|
| 000 | 00 | 00 | 00 | 100 | 00 | 00 | 10 |
| ” | ” | 01 | 01 | ” | ” | 01 | 11 |
| ” | 01 | 00 | 01 | ” | 01 | 00 | 11 |
| ” | ” | 01 | 00 | ” | ” | 01 | 10 |
| ” | 10 | 10 | 10 | ” | 10 | 10 | 00 |
| ” | ” | 11 | 11 | ” | ” | 11 | 01 |
| ” | 11 | 10 | 11 | ” | 11 | 10 | 01 |
| ” | ” | 11 | 10 | ” | ” | 11 | 00 |
| 001 | 00 | 00 | 01 | 101 | 00 | 00 | 11 |
| ” | ” | 01 | 00 | ” | ” | 01 | 10 |
| ” | 01 | 00 | 00 | ” | 01 | 00 | 10 |
| ” | ” | 01 | 01 | ” | ” | 01 | 11 |
| ” | 10 | 10 | 11 | ” | 10 | 10 | 01 |
| ” | ” | 11 | 10 | ” | ” | 11 | 00 |
| ” | 11 | 10 | 10 | ” | 11 | 10 | 00 |
| ” | ” | 11 | 11 | ” | ” | 11 | 01 |
| 010 | 00 | 10 | 00 | 110 | 00 | 10 | 10 |
| ” | ” | 11 | 01 | ” | ” | 11 | 11 |
| ” | 01 | 10 | 01 | ” | 01 | 10 | 11 |
| ” | ” | 11 | 00 | ” | ” | 11 | 10 |
| ” | 10 | 00 | 10 | ” | 10 | 00 | 00 |
| ” | ” | 01 | 11 | ” | ” | 01 | 01 |
| ” | 11 | 00 | 11 | ” | 11 | 00 | 01 |
| ” | ” | 01 | 10 | ” | ” | 01 | 00 |
| 011 | 00 | 10 | 01 | 111 | 00 | 10 | 11 |
| ” | ” | 11 | 00 | ” | ” | 11 | 10 |
| ” | 01 | 10 | 00 | ” | 01 | 10 | 10 |
| ” | ” | 11 | 01 | ” | ” | 11 | 11 |
| ” | 10 | 00 | 11 | ” | 10 | 00 | 01 |
| ” | ” | 01 | 10 | ” | ” | 01 | 00 |
| ” | 11 | 00 | 10 | ” | 11 | 00 | 00 |
| ” | ” | 01 | 11 | ” | ” | 01 | 01 |

TABLE II. The 64 possible combinations of results of Alice's public GHZ-state measurement, Alice's, Bob's, and Carol's secret Bell-state measurements on the initial state given by Eq. (24).

| Public | Alice | Bob | Carol | David |
|---|---|---|---|---|
| 0000 | 00 | 00 | 00 | 00 |
| ” | ” | 00 | 01 | 01 |
| ” | ” | 01 | 00 | 01 |
| ” | ” | 01 | 01 | 00 |
| ” | 01 | 00 | 00 | 01 |
| ” | ” | 00 | 01 | 00 |
| ” | ” | 01 | 00 | 00 |
| ” | ” | 01 | 01 | 01 |
| ” | 10 | 10 | 10 | 10 |
| ” | ” | 10 | 11 | 11 |
| ” | ” | 11 | 10 | 11 |
| ” | ” | 11 | 11 | 10 |
| ” | 11 | 10 | 10 | 11 |
| ” | ” | 10 | 11 | 10 |
| ” | ” | 11 | 10 | 10 |
| ” | ” | 11 | 11 | 11 |

TABLE III. The 16 possible combinations of results of Alice's, Bob's, Carol's, and David's secret Bell-state measurements on the initial state $|0000\rangle \otimes |00\rangle \otimes |00\rangle \otimes |00\rangle \otimes |00\rangle$, if the result of Alice's public four-qubit GHZ-state measurement is "0000".

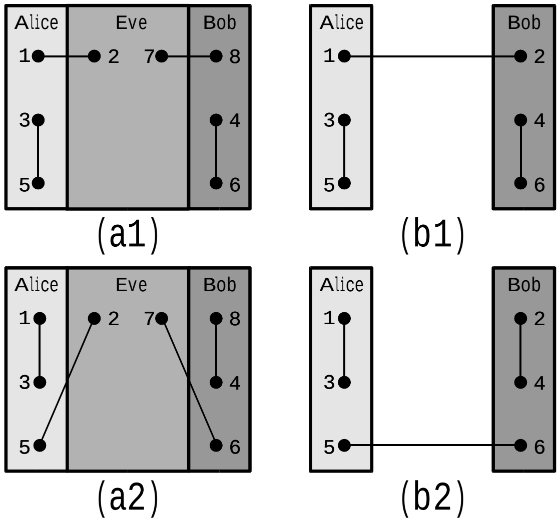


FIG. 1: (a1) and (a2) represent two steps of the protocol for two-party key distribution based on ES, assuming that Eve wants to obtain the result of Bob's secret measurement. (a1) represents the situation before Alice's and Bob's secret measurements, and (a2) the situation after these measurements. (b1) and (b2) represent, respectively, the same two steps, (a1) and (a2), but assuming that Eve is not present. Bold lines connect qubits in Bell states.

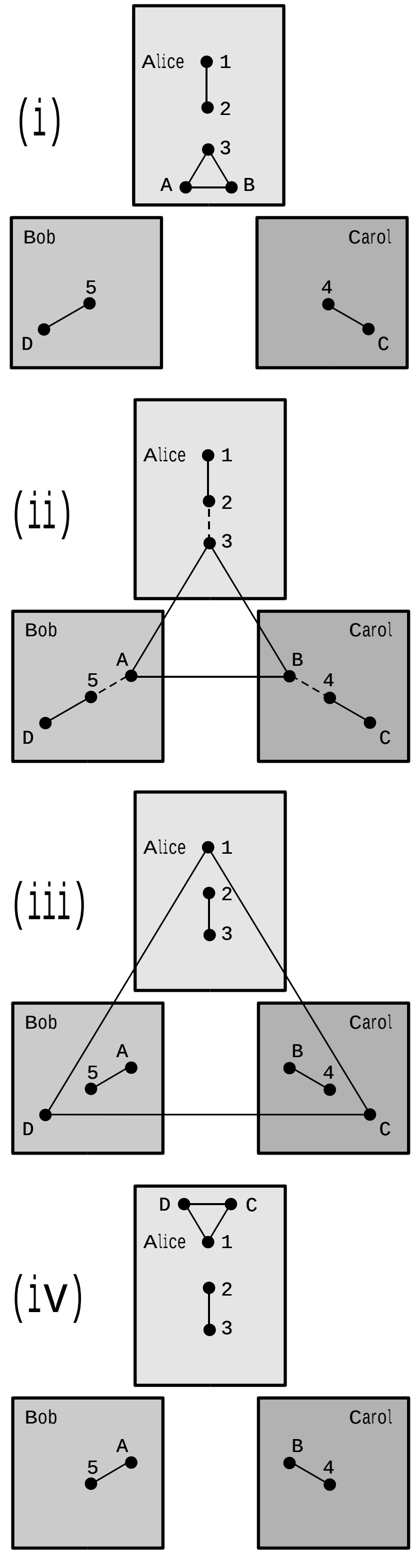


FIG.. 2: The four steps of the three-party key distribution protocol based on ES. The notation is the same introduced in Ref. [3]: triangles connect qubits in GHZ states, bold lines connect qubits in Bell states, and dashed lines represent Bell-state measurements.